

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-292

Vulnerability Summary for the Week of October 12, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
achieveo -- achieveo	SQL injection vulnerability in the get_employee function in classweekreport.inc in Achievo before 1.4.0 allows remote attackers to execute arbitrary SQL commands via the userid parameter (aka user_id variable) to dispatch.php.	2009-10-16	7.5	CVE-2009-2734 CONFIRM
achieveo -- achieveo	PHP remote file inclusion vulnerability in debugger.php in Achievo before 1.4.0 allows remote attackers to execute arbitrary PHP code via a URL in the config_atkroot parameter.	2009-10-16	7.5	CVE-2009-3705 CONFIRM
adobe -- acrobat adobe -- reader	Unspecified vulnerability in Adobe Reader and Acrobat 9.1.3 and earlier, and possibly 7.1.3 and 8.1.6, allows remote attackers to execute arbitrary code via a crafted PDF file that triggers memory corruption, as exploited in the wild in October 2009. NOTE: some of these details are obtained from third party information.	2009-10-13	9.3	CVE-2009-3459 CONFIRM

battleblog -- battle_blog	SQL injection vulnerability in admin/authenticate.asp in Battle Blog 1.25 and 1.30 build 2 allows remote attackers to execute arbitrary SQL commands via the UserName parameter.	2009-10-16	7.5	CVE-2009-3718 BID OSVDB MILWoRM SECUNIA MISC
ca -- anti-virus ca -- anti-virus_for_the_enterprise ca -- anti-virus_gateway ca -- anti-virus_plus ca -- anti-virus_sdk ca -- arcserve_backup ca -- arcserve_for_windows_client_agent ca -- arcserve_for_windows_server_component ca -- common_services ca -- etrust_anti-virus_gateway ca -- etrust_anti-virus_sdk ca -- etrust_antivirus ca -- etrust_ez_antivirus ca -- etrust_integrated_threat_management ca -- etrust_intrusion_detection ca -- etrust_secure_content_manager ca -- gateway_security ca -- internet_security_suite ca -- internet_security_suite_2008 ca -- internet_security_suite_plus_2008 ca -- internet_security_suite_plus_2009 ca -- network_and_systems_management ca -- protection_suites ca -- secure_content_manager ca -- threat_manager ca -- threat_manager_total_defense ca -- unicenter_network_and_systems_management	Unspecified vulnerability in the arclib component in the Anti-Virus engine in CA Anti-Virus for the Enterprise (formerly eTrust Antivirus) 7.1 through r8.1; Anti-Virus 2007 (v8) through 2009; eTrust EZ Antivirus r7.1; Internet Security Suite 2007 (v3) through Plus 2009; and other CA products allows remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted RAR archive file that triggers heap corruption, a different vulnerability than CVE-2009-3588.	2009-10-13	9.3	CVE-2009-3587 CONFIRM
cisco -- unified_presence_server	The TimesTenD process in Cisco Unified Presence 1.x, 6.x before 6.0(6), and 7.x before 7.0(4) allows remote attackers to cause a denial of service (process crash) via a large number of TCP connections to ports 16200 and 22794, aka Bug ID CSCsy17662.	2009-10-16	7.8	CVE-2009-2874 CISCO
hp -- loadrunner persits -- xupload	Directory traversal vulnerability in the Persits.XUpload.2 ActiveX control (XUpload.ocx) in HP LoadRunner 9.5 allows remote attackers to create arbitrary files via \.. (backwards slash dot dot) sequences in the third argument to the MakeHttpRequest method.	2009-10-13	9.3	CVE-2009-3693 SECUNIA MISC
ibm -- informix_client_sdk ibm -- informix_connect_runtime	Multiple integer overflows in setnet32.exe 3.50.0.13752 in IBM Informix Client SDK 3.0 and 3.50 and Informix Connect Runtime 3.x allow remote attackers to execute arbitrary code via a .nfx file with a crafted (1) HostSize, and possibly (2) ProtoSize and (3) ServerSize, field that triggers a stack-based	2009-10-13	9.3	CVE-2009-3691 XF VUPEN BID OSVDB SECTRACK

	buffer overflow involving a crafted HostList field. NOTE: some of these details are obtained from third party information.			SECUNIA MISC
ibm -- vios ibm -- aix	Stack-based buffer overflow in libcsa.a (aka the calendar daemon library) in IBM AIX 5.x through 5.3.10 and 6.x through 6.1.3, and VIOS 2.1 and earlier, allows remote attackers to execute arbitrary code via a long XDR string in the first argument to procedure 21 of rpc.cmsd.	2009-10-15	10.0	CVE-2009-3699 VUPEN BID IDEFENSE
justclone -- ebay_clone	Multiple SQL injection vulnerabilities in Ebay Clone 2009 allow remote attackers to execute arbitrary SQL commands via the (1) user_id parameter to feedback.php; and the item_id parameter to (2) view_full_size.php, (3) classifide_ad.php, and (4) crosspromoteitems.php.	2009-10-16	7.5	CVE-2009-3712 XF MILWORM SECUNIA
konae -- alleycode_html_editor	Stack-based buffer overflow in the Meta Content Optimizer in Konae Technologies Alleycode HTML Editor 2.21 allows user-assisted remote attackers to execute arbitrary code via a long value in a (1) description or (2) keyword META tag. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-10-16	9.3	CVE-2009-3708 SECUNIA OSVDB
konae -- alleycode_html_editor	Stack-based buffer overflow in the Meta Content Optimizer in Konae Technologies Alleycode HTML Editor 2.21 allows user-assisted remote attackers to execute arbitrary code via a long value in a TITLE tag.	2009-10-16	9.3	CVE-2009-3709 BUGTRAQ SECUNIA MISC OSVDB
lucivil -- patplayer	Heap-based buffer overflow in LucVil PatPlayer 3.9 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long URI in a playlist (.m3u) file.	2009-10-16	9.3	CVE-2009-3717 XF VUPEN MILWORM SECUNIA OSVDB
microsoft -- .net_framework microsoft -- windows_2000 microsoft -- windows_7 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft .NET Framework 1.0 SP3, 1.1 SP1, and 2.0 SP1 does not properly validate .NET verifiable code, which allows remote attackers to obtain unintended access to stack memory, and execute arbitrary code, via (1) a crafted XAML browser application (XBAP), (2) a crafted ASP.NET application, or (3) a crafted .NET	2009-10-14	9.3	CVE-2009-0090 MS

	Framework application, aka "Microsoft .NET Framework Pointer Verification Vulnerability."			
microsoft -- .net_framework microsoft -- windows_2000 microsoft -- windows_7 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft .NET Framework 2.0, 2.0 SP1, and 3.5 does not properly enforce a certain type-equality constraint in .NET verifiable code, which allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP), (2) a crafted ASP.NET application, or (3) a crafted .NET Framework application, aka "Microsoft .NET Framework Type Verification Vulnerability."	2009-10-14	9.3	CVE-2009-0091 MS
microsoft -- windows_media_format_runtime microsoft -- windows_media_player microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Windows Media Runtime, as used in DirectShow WMA Voice Codec, Windows Media Audio Voice Decoder, and Audio Compression Manager (ACM), does not properly process Advanced Systems Format (ASF) files, which allows remote attackers to execute arbitrary code via a crafted audio file that uses the Windows Media Speech codec, aka "Windows Media Runtime Voice Sample Rate Vulnerability."	2009-10-14	9.3	CVE-2009-0555 MS
microsoft -- internet_explorer microsoft -- windows_2000 microsoft -- windows_7 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Unspecified vulnerability in Microsoft Internet Explorer 5.01 SP4, 6, 6 SP1, and 7 allows remote attackers to execute arbitrary code via a crafted data stream header that triggers memory corruption, aka "Data Stream Header Corruption Vulnerability."	2009-10-14	9.3	CVE-2009-1547 MS
microsoft -- .net_framework microsoft -- windows_2000 microsoft -- windows_7 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	The Common Language Runtime (CLR) in Microsoft .NET Framework 2.0, 2.0 SP1, 2.0 SP2, 3.5, and 3.5 SP1, and Silverlight 2, does not properly handle interfaces, which allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP), (2) a crafted Silverlight application, (3) a crafted ASP.NET application, or (4) a crafted .NET Framework application, aka "Microsoft Silverlight and Microsoft .NET Framework CLR Vulnerability."	2009-10-14	9.3	CVE-2009-2497 MS
microsoft -- .net_framework microsoft -- excel_viewer microsoft -- expression_web microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office microsoft -- office_compatibility_pack microsoft -- office_excel_viewer	Integer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3,			

microsoft -- office_groove microsoft -- office_powerpoint_viewer microsoft -- office_word_viewer microsoft -- platform_sdk microsoft -- project microsoft -- report_viewer microsoft -- sql_server microsoft -- sql_server_reporting_services microsoft -- visio microsoft -- visual_foxpro microsoft -- visual_studio microsoft -- visual_studio_net microsoft -- word_viewer microsoft -- works microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted WMF image file, aka "GDI+ WMF Integer Overflow Vulnerability."	2009-10-14	9.3	CVE-2009-2500 MS
microsoft -- .net_framework microsoft -- excel_viewer microsoft -- expression_web microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office microsoft -- office_compatibility_pack microsoft -- office_excel_viewer microsoft -- office_groove microsoft -- office_powerpoint_viewer microsoft -- office_word_viewer microsoft -- platform_sdk microsoft -- project microsoft -- report_viewer microsoft -- sql_server microsoft -- sql_server_reporting_services microsoft -- visio microsoft -- visual_foxpro microsoft -- visual_studio microsoft -- visual_studio_net microsoft -- word_viewer microsoft -- works microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Heap-based buffer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted PNG image file, aka "GDI+ PNG Heap Overflow Vulnerability."	2009-10-14	9.3	CVE-2009-2501 MS
microsoft -- .net_framework microsoft -- excel_viewer microsoft -- expression_web microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office microsoft -- office_compatibility_pack microsoft -- office_excel_viewer microsoft -- office_groove microsoft -- office_powerpoint_viewer microsoft -- office_word_viewer microsoft -- platform_sdk microsoft -- project microsoft -- report_viewer microsoft -- sql_server microsoft -- sql_server_reporting_services	Buffer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007	2009-10-14	9.3	CVE-2009-2502 MS

microsoft -- visio microsoft -- visual_foxpro microsoft -- visual_studio microsoft -- visual_studio_.net microsoft -- word_viewer microsoft -- works microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted TIFF image file, aka "GDI+ TIFF Buffer Overflow Vulnerability."			
microsoft -- .net_framework microsoft -- excel_viewer microsoft -- expression_web microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office microsoft -- office_compatibility_pack microsoft -- office_excel_viewer microsoft -- office_groove microsoft -- office_powerpoint_viewer microsoft -- office_word_viewer microsoft -- platform_sdk microsoft -- project microsoft -- report_viewer microsoft -- sql_server microsoft -- sql_server_reporting_services microsoft -- visio microsoft -- visual_foxpro microsoft -- visual_studio microsoft -- visual_studio_.net microsoft -- word_viewer microsoft -- works microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Windows Server 2003 SP2, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 does not properly allocate an unspecified buffer, which allows remote attackers to execute arbitrary code via a crafted TIFF image file that triggers memory corruption, aka "GDI+ TIFF Memory Corruption Vulnerability."	2009-10-14	9.3	CVE-2009-2503 MS
microsoft -- .net_framework microsoft -- excel_viewer microsoft -- expression_web microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office microsoft -- office_compatibility_pack microsoft -- office_excel_viewer microsoft -- office_groove microsoft -- office_powerpoint_viewer microsoft -- office_word_viewer microsoft -- platform_sdk microsoft -- project microsoft -- report_viewer microsoft -- sql_server microsoft -- sql_server_reporting_services microsoft -- visio	Multiple integer overflows in unspecified APIs in GDI+ in Microsoft .NET Framework 1.1 SP1, .NET Framework 2.0 SP1 and SP2, Windows XP SP2 and SP3, Windows Server 2003 SP2, Vista Gold and SP1, Server 2008 Gold, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5	2009-10-14	9.3	CVE-2009-2504 MS

microsoft -- visual_foxpro microsoft -- visual_studio microsoft -- visual_studio_dotnet microsoft -- word_viewer microsoft -- works microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	200 / Gold and SP1, WORKS 0.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allow remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP), (2) a crafted ASP.NET application, or (3) a crafted .NET Framework application, aka "GDI+ .NET API Vulnerability."			
microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_xp	A certain ActiveX control in the Indexing Service in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly process URLs, which allows remote attackers to execute arbitrary programs via unspecified vectors that cause a "vulnerable binary" to load and run, aka "Memory Corruption in Indexing Service Vulnerability."	2009-10-14	9.3	CVE-2009-2507 MS
microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_7 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	The CryptoAPI component in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, as used by Internet Explorer and other applications, does not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, aka "Null Truncation in X.509 Common Name Vulnerability," a related issue to CVE-2009-2408.	2009-10-14	7.5	CVE-2009-2510 MS
microsoft -- windows_2000 microsoft -- windows_7 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Integer overflow in the CryptoAPI component in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows man-in-the-middle attackers to spoof arbitrary SSL servers and other entities via an X.509 certificate that has a malformed ASN.1 Object Identifier (OID) and was issued by a legitimate Certification Authority, aka "Integer Overflow in X.509 Object Identifiers Vulnerability."	2009-10-14	7.5	CVE-2009-2511 MS

microsoft -- .net_framework microsoft -- 20007_office_system microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office microsoft -- office_compatibility_pack_for_word_excel_ppt_2007 microsoft -- office_excel_viewer microsoft -- office_groove microsoft -- office_powerpoint microsoft -- office_project microsoft -- office_visio microsoft -- office_word_viewer microsoft -- office_xp microsoft -- report_viewer microsoft -- sql_server microsoft -- works microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Integer overflow in GDI+ in Microsoft Office XP SP3 allows remote attackers to execute arbitrary code via an Office document with a bitmap (aka BMP) image that triggers memory corruption, aka "Office BMP Integer Overflow Vulnerability."	2009-10-14	9.3	CVE-2009-2518 MS
microsoft -- windows_2003_server microsoft -- windows_7 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Integer underflow in the NTLM authentication feature in the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote attackers to cause a denial of service (reboot) via a malformed packet, aka "Local Security Authority Subsystem Service Integer Overflow Vulnerability."	2009-10-14	7.8	CVE-2009-2524 MS
microsoft -- windows_media_format_runtime microsoft -- windows_media_player microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Windows Media Runtime, as used in DirectShow WMA Voice Codec, Windows Media Audio Voice Decoder, and Audio Compression Manager (ACM), does not properly initialize unspecified functions within compressed audio files, which allows remote attackers to execute arbitrary code via (1) a crafted media file or (2) crafted streaming content, aka "Windows Media Runtime Heap Corruption Vulnerability."	2009-10-14	9.3	CVE-2009-2525 MS
microsoft -- windows_server_2008 microsoft -- windows_vista	Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 do not properly validate fields in SMBv2 packets, which allows remote attackers to cause a denial of service (infinite loop and system hang) via a crafted packet to the Server service, aka "SMBv2 Infinite Loop"	2009-10-14	7.8	CVE-2009-2526 MS

	Vulnerability."			
microsoft -- windows_media_player microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_xp	Heap-based buffer overflow in Microsoft Windows Media Player 6.4 allows remote attackers to execute arbitrary code via (1) a crafted ASF file or (2) crafted streaming content, aka "WMP Heap Overflow Vulnerability."	2009-10-14	9.3	CVE-2009-2527 MS
microsoft -- .net_framework microsoft -- excel_viewer microsoft -- expression_web microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office microsoft -- office_compatibility_pack microsoft -- office_excel_viewer microsoft -- office_groove microsoft -- office_powerpoint_viewer microsoft -- office_word_viewer microsoft -- platform_sdk microsoft -- project microsoft -- report_viewer microsoft -- sql_server microsoft -- sql_server_reporting_services microsoft -- visio microsoft -- visual_foxpro microsoft -- visual_studio microsoft -- visual_studio_.net microsoft -- word_viewer microsoft -- works microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	GDI+ in Microsoft Office XP SP3 does not properly handle malformed objects in Office Art Property Tables, which allows remote attackers to execute arbitrary code via a crafted Office document that triggers memory corruption, aka "Memory Corruption Vulnerability."	2009-10-14	9.3	CVE-2009-2528 MS
microsoft -- internet_explorer microsoft -- windows_2000 microsoft -- windows_7 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Internet Explorer 5.01 SP4, 6, 6 SP1, 7, and 8 does not properly handle argument validation for unspecified variables, which allows remote attackers to execute arbitrary code via a crafted HTML document, aka "HTML Component Handling Vulnerability."	2009-10-14	9.3	CVE-2009-2529 MS
microsoft -- internet_explorer microsoft -- windows_2000 microsoft -- windows_7 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Internet Explorer 6, 6 SP1, 7, and 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability," a different vulnerability than CVE-2009-2531.	2009-10-14	9.3	CVE-2009-2530 MS
microsoft -- internet_explorer	Microsoft Internet Explorer 6, 6 SP1, 7, and 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability," a different vulnerability than CVE-2009-2531.			

microsoft -- windows_2000 microsoft -- windows_7 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability," a different vulnerability than CVE-2009-2530.	2009-10-14	9.3	CVE-2009-2531 MS
microsoft -- windows_server_2008 microsoft -- windows_vista	Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC do not properly process the command value in an SMB Multi-Protocol Negotiate Request packet, which allows remote attackers to execute arbitrary code via a crafted SMBv2 packet to the Server service, aka "SMBv2 Command Value Vulnerability."	2009-10-14	10.0	CVE-2009-2532 MS
microsoft -- .net_framework microsoft -- excel_viewer microsoft -- expression_web microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office microsoft -- office_compatibility_pack microsoft -- office_excel_viewer microsoft -- office_groove microsoft -- office_powerpoint_viewer microsoft -- office_word_viewer microsoft -- platform_sdk microsoft -- project microsoft -- report_viewer microsoft -- sql_server microsoft -- sql_server_reporting_services microsoft -- visio microsoft -- visual_foxpro microsoft -- visual_studio microsoft -- visual_studio_.net microsoft -- word_viewer microsoft -- works microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Integer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted PNG image file, aka "GDI+ PNG Integer Overflow Vulnerability."	2009-10-14	9.3	CVE-2009-3126 MS
morcego_cms -- morcego_cms	SQL injection vulnerability in fichero.php in MorcegoCMS 1.7.6 and earlier allows remote attackers to execute arbitrary SQL commands via the query string.	2009-10-16	7.5	CVE-2009-3713 XF MILWoRM SECUNIA OSVDB
nbnmuadmin nbnmuadmin	SQL injection vulnerability in the PDF schema generator functionality in phpMyAdmin 2.11.x before 2.11.9.6 and 3.x	2009-10-	--	CVE-2009-3697 FEDORA CONFIRM XF VUPEN CERTDM

sun -- sunos	before 3.2.2.1 allows remote attackers to execute arbitrary SQL commands via unspecified interface parameters.	16	/•5	CONFIRM MANDRIVA SECUNIA MLIST MLIST CONFIRM CONFIRM CONFIRM
sun -- virtualbox	Unspecified vulnerability in the VBoxNetAdpCtl configuration tool in Sun VirtualBox 3.0.x before 3.0.8 on Solaris x86, Linux, and Mac OS X allows local users to gain privileges via unknown vectors.	2009-10-13	7.2	CVE-2009-3692 SUNALERT
unbound -- unbound	Unbound before 1.3.4 does not properly verify signatures for NSEC3 records, which allows remote attackers to cause secure delegations to be downgraded via DNS spoofing or other DNS-related attacks in conjunction with crafted delegation responses.	2009-10-13	7.5	CVE-2009-3602 XF VUPEN MLIST MLIST MLIST SECUNIA OSVDB
vmware -- fusion	The vmx86 kernel extension in VMware Fusion before 2.0.6 build 196839 does not use correct file permissions, which allows host OS users to gain privileges on the host OS via unspecified vectors.	2009-10-16	10.0	CVE-2009-3281 VUPEN CONFIRM SECTRACK SECUNIA MLIST
vmware -- fusion	Integer overflow in the vmx86 kernel extension in VMware Fusion before 2.0.6 build 196839 allows host OS users to cause a denial of service to the host OS via unspecified vectors.	2009-10-16	7.8	CVE-2009-3282 VUPEN CONFIRM SECTRACK SECUNIA MLIST

[Back to top](#)**Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
316solutions -- boost	Unspecified vulnerability in Boost before 6.x-1.03, a module for Drupal, allows remote attackers to create new webroot directories via unknown attack vectors.	2009-10-09	6.4	CVE-2009-3654 CONFIRM CONFIRM
achieveo -- achieveo	Multiple cross-site scripting (XSS) vulnerabilities in Achievo before 1.4.0 allow remote attackers to inject arbitrary web script or HTML via (1) the scheduler title in the scheduler module, and the (2) atksearch[contractnumber], (3) atksearch_AE_customer[customer], (4) atksearchmode[contracttype], and possibly (5) atksearch[contractname]	2009-10-16	4.3	CVE-2009-2733 CONFIRM

	parameters to the Organization Contracts administration page, reachable through dispatch.php.			
android -- android	The com.android.phone process in Android 1.5 CRBxx allows remote attackers to cause a denial of service (application restart and network disconnection) via an SMS message containing a malformed WAP Push message that triggers an ArrayIndexOutOfBoundsException exception, possibly a related issue to CVE-2009-2656.	2009-10-14	4.3	CVE-2009-2999 XF BUGTRAQ MISC SECTRACK CONFIRM
android -- android	An unspecified function in the Dalvik API in Android 1.5 and earlier allows remote attackers to cause a denial of service (system process restart) via a crafted application, possibly a related issue to CVE-2009-2656.	2009-10-14	4.3	CVE-2009-3698 XF BID BUGTRAQ MISC SECTRACK MISC
apache -- apr apache -- http_server	The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.	2009-10-13	5.0	CVE-2009-2699 BID
battleblog -- battle_blog	Cross-site scripting (XSS) vulnerability in comment.asp in Battle Blog 1.25 and 1.30 build 2 allows remote attackers to inject arbitrary web script or HTML via a comment.	2009-10-16	4.3	CVE-2009-3719 XF BID MILWORM SECUNIA MISC
ca -- anti-virus ca -- anti-virus_for_the_enterprise ca -- anti-virus_gateway ca -- anti-virus_plus ca -- anti-virus_sdk ca -- arcserve_backup ca -- arcserve_for_windows_client_agent ca -- arcserve_for_windows_server_component ca -- common_services ca -- etrust_anti-virus_gateway ca -- etrust_anti-virus_sdk ca -- etrust_antivirus ca -- etrust_ez_antivirus ca -- etrust_integrated_threat_management ca -- etrust_intrusion_detection ca -- etrust_secure_content_manager ca -- gateway_security ca -- internet_security_suite ca -- internet_security_suite_2008	Unspecified vulnerability in the arclib component in the Anti-Virus engine in CA Anti-Virus for the Enterprise (formerly eTrust Antivirus) 7.1 through r8.1; Anti-Virus 2007 (v8) through 2009; eTrust EZ Antivirus r7.1; Internet Security Suite 2007 (v3) through Plus 2009; and other CA products allows remote attackers to cause a denial of service via a crafted RAR archive file that triggers stack corruption, a different vulnerability.	2009-10-13	4.3	CVE-2009-3588 VUPEN CONFIRM

ca -- internet_security_suite_plus_2008 ca -- internet_security_suite_plus_2009 ca -- network_and_systems_management ca -- protection_suites ca -- secure_content_manager ca -- threat_manager ca -- threat_manager_total_defense ca -- unicenter_network_and_systems_management	corruption, a different vulnerability than CVE-2009-3587.			
djangoproject -- django	Algorithmic complexity vulnerability in the forms library in Django 1.0 before 1.0.4 and 1.1 before 1.1.1 allows remote attackers to cause a denial of service (CPU consumption) via a crafted (1) EmailField (email address) or (2) URLField (URL) that triggers a large amount of backtracking in a regular expression.	2009-10-13	5.0	CVE-2009-3695 VUPEN BID CONFIRM
hp -- cm8050_mfp hp -- cm8060_mfp hp -- color_laserjet_300on hp -- color_laserjet_360on hp -- color_laserjet_380on hp -- color_laserjet_4700n hp -- color_laserjet_4730_mfp hp -- color_laserjet_6040_mfp hp -- color_laserjet_cm4730_mfp hp -- color_laserjet_cp3505 hp -- color_laserjet_cp4005n hp -- color_laserjet_cp6015 hp -- ds_9200c hp -- ds_9250c hp -- laserjet_2410 hp -- laserjet_2420 hp -- laserjet_2430n hp -- laserjet_4240 hp -- laserjet_4250n hp -- laserjet_4345_mfp hp -- laserjet_4350n hp -- laserjet_5200n hp -- laserjet_9040_mfp hp -- laserjet_9040n hp -- laserjet_9050_mfp hp -- laserjet_9050n hp -- laserjet_m3027_mfp hp -- laserjet_m3035_mfp hp -- laserjet_m4345x_mfp hp -- laserjet_m5025_mfp hp -- laserjet_m9040_mpf hp -- laserjet_m9050_mpf hp -- laserjet_p3005n hp -- laserjet_p4014 hp -- laserjet_p4515	Multiple cross-site scripting (XSS) vulnerabilities in Jetdirect and the Embedded Web Server (EWS) on certain HP LaserJet and Color LaserJet printers, and HP Digital Senders, allow remote attackers to inject arbitrary web script or HTML via the (1) Product_URL or (2) Tech_URL parameter in an Apply action to the support_param.html/config script.	2009-10-13	4.3	CVE-2009-2684 XF VUPEN BID BUGTRAQ SECUNIA HP HP MISC
jdtmmsm -- ezrecipe-zee	Directory traversal vulnerability in config/config.php in ezRecipe-Zee 91, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the cfg[prePath]	2009-10-13	6.8	CVE-2009-3694 XF MISC SECUNIA OSVDB

	parameter.		OSVDB
linux -- kernel	The d_delete function in fs/ecryptfs/inode.c in eCryptfs in the Linux kernel 2.6.31 allows local users to cause a denial of service (kernel OOPS) and possibly execute arbitrary code via unspecified vectors that cause a "negative dentry" and trigger a NULL pointer dereference, as demonstrated via a Mutt temporary directory in an eCryptfs mount.	2009-10-13	4.9 CVE-2009-2908 BID
maniacomputer -- mcshoutbox	Cross-site scripting (XSS) vulnerability in admin_login.php in MCshoutbox 1.1 allows remote attackers to inject arbitrary web script or HTML via the loginerror parameter.	2009-10-16	4.3 CVE-2009-3714 XF VUPEN MILWORM SECUNIA OSVDB
maniacomputer -- mcshoutbox	Multiple SQL injection vulnerabilities in scr_login.php in MCshoutbox 1.1, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters.	2009-10-16	6.8 CVE-2009-3715 XF VUPEN MILWORM SECUNIA OSVDB
maniacomputer -- mcshoutbox	Unrestricted file upload vulnerability in admin.php in MCshoutbox 1.1 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in smilies/.	2009-10-16	6.5 CVE-2009-3716 XF MILWORM SECUNIA OSVDB
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Integer underflow in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows local users to gain privileges via a crafted application that triggers an incorrect truncation of a 64-bit integer to a 32-bit integer, aka "Windows Kernel Integer Underflow Vulnerability."	2009-10-14	6.8 CVE-2009-2515 MS
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold and SP1, and Server 2008 Gold does not properly validate data sent from user mode, which allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, aka "Windows Kernel NULL Pointer Dereference Vulnerability."	2009-10-14	6.8 CVE-2009-2516 MS
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008	The kernel in Microsoft Windows Server 2003 SP2 does not properly handle unspecified exceptions when an error condition occurs, which allows local users to cause a denial of	2009-10-14	4.6 CVE-2009-2517

microsoft -- windows_vista microsoft -- windows_xp	allows local users to cause a crash or service (reboot) via a crafted application, aka "Windows Kernel Exception Handler Vulnerability."	14		MS
phpmyadmin -- phpmyadmin	Cross-site scripting (XSS) vulnerability in phpMyAdmin 2.11.x before 2.11.9.6 and 3.x before 3.2.2.1 allows remote attackers to inject arbitrary web script or HTML via a crafted name for a MySQL table.	2009-10-16	4.3	CVE-2009-3696 FEDORA FEDORA CONFIRM XF VUPEN CONFIRM MANDRIVA SECUNIA MLIST MLIST CONFIRM CONFIRM CONFIRM
springsource -- application_management_suite springsource -- hyperic_hq springsource -- tc_server	Multiple cross-site scripting (XSS) vulnerabilities in hq/web/common/GenericError.jsp in the generic exception handler in the web interface in SpringSource Hyperic HQ 3.2.x before 3.2.6.1, 4.0.x before 4.0.3.1, 4.1.x before 4.1.2.1, and 4.2-beta1; Application Management Suite (AMS) 2.0.0.SR3; and tc Server 6.0.20.B allow remote attackers to inject arbitrary web script or HTML via invalid values for numerical parameters, as demonstrated by an uncaught java.lang.NumberFormatException exception resulting from (1) the typeId parameter to mastheadAttach.do, (2) the eid parameter to Resource.do, and (3) the u parameter in a view action to admin/user/UserAdmin.do. NOTE: some of these details are obtained from third party information.	2009-10-13	4.3	CVE-2009-2897 CONFIRM BUGTRAQ BUGTRAQ MISC MISC
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the ZFS filesystem in Sun Solaris 10, and OpenSolaris snv_100 through snv_117, allows local users to bypass intended limitations of the file_chown_self privilege via certain uses of the chown system call.	2009-10-16	4.4	CVE-2009-3706 SUNALERT CONFIRM
symantec -- securityexpressions_audit_and_compliance_server	Cross-site scripting (XSS) vulnerability in Symantec SecurityExpressions Audit and Compliance Server 4.1.1, 4.1, and earlier allows remote attackers to inject arbitrary web script or HTML via vectors that trigger an error message in a response, related to an "HTML Injection issue."	2009-10-15	4.3	CVE-2009-3030 CONFIRM BID
	VMware Authentication Daemon 1.0			

vmware -- ace vmware -- player vmware -- workstation	in vmware-authd.exe 6.5.3.8888 in the VMware Authorization Service 2.5.3 and earlier in VMware Workstation 6.5.3 build 185404, VMware Player 2.5.2 build 156735 and 2.5.3 build 185404, and VMware ACE 2.5.3 allows remote attackers to cause a denial of service (process crash) via a \x25\xFF sequence in the USER and PASS commands, related to a "format string DoS" issue. NOTE: some of these details are obtained from third party information.	2009-10-16	5.0	CVE-2009-3707 MISC MISC SECTRACK SECUNIA
--	---	------------	-----	--

[Back to top](#)**Low Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
springsource -- application_management_suite springsource -- hyperic_hq springsource -- tc_server	Cross-site scripting (XSS) vulnerability in the Alerts list feature in the web interface in SpringSource Hyperic HQ 3.2.x before 3.2.6.1, 4.0.x before 4.0.3.1, 4.1.x before 4.1.2.1, and 4.2-beta1; Application Management Suite (AMS) 2.0.0.SR3; and tc Server 6.0.20.B allows remote authenticated users to inject arbitrary web script or HTML via the Description field. NOTE: some of these details are obtained from third party information.	2009-10-13	3.5	CVE-2009-2898 CONFIRM MISC MISC
symantec -- securityexpressions_audit_and_compliance_server	Cross-site scripting (XSS) vulnerability in the console in Symantec SecurityExpressions Audit and Compliance Server 4.1.1, 4.1, and earlier allows remote authenticated users to inject arbitrary web script or HTML via "external client input" that triggers crafted error messages.	2009-10-15	3.5	CVE-2009-3029 CONFIRM BID

[Back to top](#)**Last updated October 19, 2009**
 Print This Document